ASEC Report 11월

® ASEC Report

2004. 12

안철수연구소의 시큐리티대응센터(Ahnlab Security E-response Center)는 악성코드 및 보안위협으로부터 고객을 안전하게 지키기 위하여 바이러스와 보안 전문가들로 구성되어 있는 조직이다.

이 리포트는 ㈜안철수연구소의 ASEC에서 국내 인터넷 보안과 고객에게 보다 다양한 정보를 제공하기 위하여 바이러스와 시큐리티의 종합된 정보를 매월 요약하여 리포트 형태로 제공하고 있다.

SUMMARY

취약점에 대한 패치가 발표되기 전에 발견, 확산된 보프라 웜 …

11월에도 지난달과 마찬가지로 V3의 진단기능이 강화됨에 따라 악성코드의 피해신고와 신종 발견 건수가 지난달에 이어 이번달에도 감소추세를 보였다. 특히 피해신고된 악성코드의 수는 올 1월 이후 최저치를 나타내고 있다.

11월에는 인터넷 익스플로러 6.0 SP1의 IFRAME SRC NAME 버퍼오버플로우 취약점이 발견되었다. 이 취약점은 발견된지 4일만에 보프라 웜의 전파경로로 사용되어 전파되었고, 그 후 약 20일 이후인 12월 1일에 해당 취약점에 대한 패치가 발표되었다. 이처럼 취약점 발견 후 이 취약점을 이용한 악성코드 발견까지의 시간이 매우 짧아지고 있어 해당 취약점에 대한 예방책도 없이 피해가 급속히 확산될 수 있음을 보여주는 한 예라 할 수 있다.

11월에는 보프라 웜 외에도 심비안 OS에서 실행되는 스컬스가 발견되었다. 스컬스의 확산력이 높지 않고 심비안 OS가 한국에서는 널리 사용되지 않기 때문에 아직까지는 큰 피해가 없으나, 올해 들어 모바일용 악성코드의 발견이 간혹되는 것으로 미루어, 앞으로는 모바일 악성코드의 피해가 확산될 수 있음을 미루어 짐작해 볼 수 있다.

일본은 여전히 넷스카이 웜이 강세를 보이며 지난달과 비슷한 양상을 보이고 있다. 반면에 중국은 백쯔 웜의 피해가 증가하여, 오랫동안 강세를 보여온 넷스카이 웜이나 러브게이트 웜의 수준과 비슷한 피해를 보였다. 또한 트로이목마나 백도어류의 발견이 많았던 기존의 추세에서 벗어나 QQ 메신저 관련 트로이목마의 변형과 애드웨어류가 수적으로 크게 증가한 것이 큰 특징이라 하겠다.

I. 11월 악성코드 피해 Top 10

작성자 : 박태환 연구원(juun5@ahnlab.com)

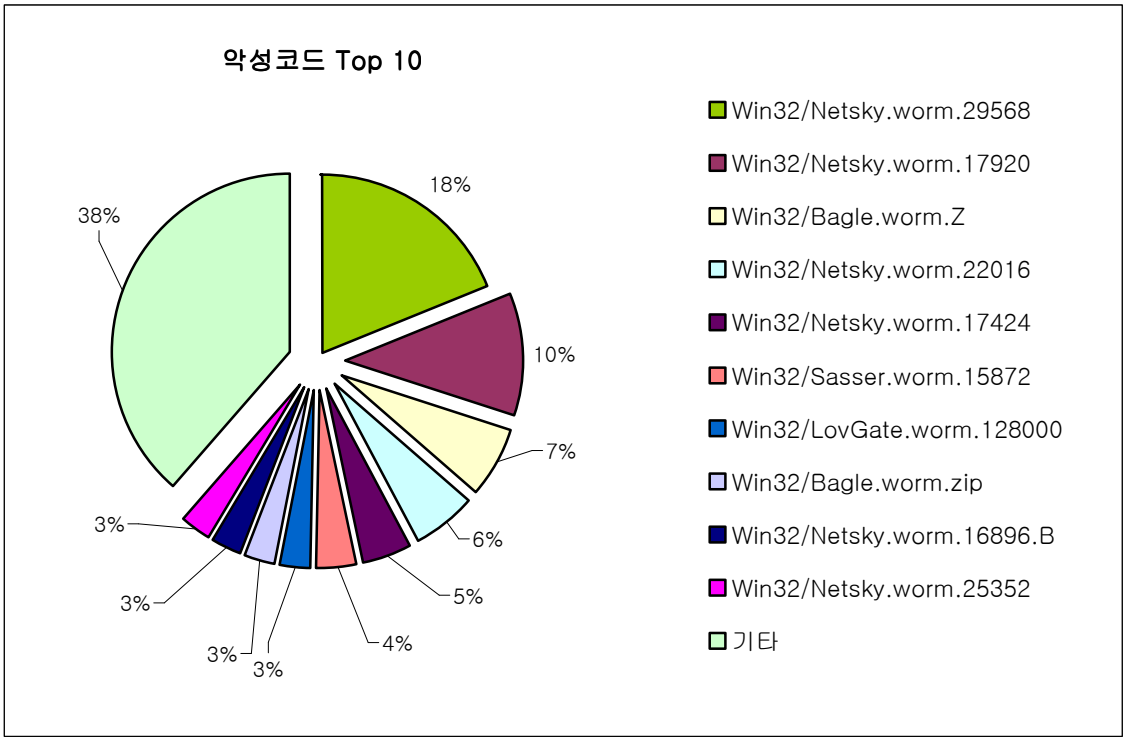
순위		악성코드명	건수	%
1	-	Win32/Netsky.worm.29568	494	18.9%
2	-	Win32/Netsky.worm.17920	289	11.0%
3	-	Win32/Bagle.worm.Z	174	6.6%
4	2↑	Win32/Netsky.worm.22016	148	5.6%
5	-	Win32/Netsky.worm.17424	121	4.6%
6	1↑	Win32/Sasser.worm.15872	92	3.5%
7	2↑	Win32/LovGate.worm.128000	74	2.8%
8	New	Win32/Bagle.worm.zip	72	2.7%
9	5↓	Win32/Netsky.worm.16896.B	72	2.7%
10	2↓	Win32/Netsky.worm.25352	71	2.7%
		기타	1,013	38.7%
합 계			2,620	100

[표1] 2004년 11월 악성코드 피해 Top 10

11월 악성코드 피해 동향

바이러스, 웜, 트로이목마 등의 11월 악성코드 피해 건수는 9월 3,910건, 10월 3,199건으로 점차 감소하는 추세를 보이기 시작하더니 11월 2,620 건으로, 역시 감소추세를 보였다. 피해집계 및 악성코드 종류가 계속 감소한 것은 V3엔진의 악성 아이알씨봇(IRCBot)류에 대한 진단/치료(삭제) 기능이 강화된 것이 주된 이유로 판단된다. 따라서 이를 전반적인 악성코드의 수가 감소한 것으로 해석하는 것에는 무리가 있다. 전반적인 감소세에 따라 11월 악성코드 피해 Top 10의 순위에 다소 변화가 있었다. 넷스카이 웜, 베이글 웜, 새서 웜, 러브게이트 웜 변종들이 항상 수위를 차지하고 있는 것을 볼 수 있다.

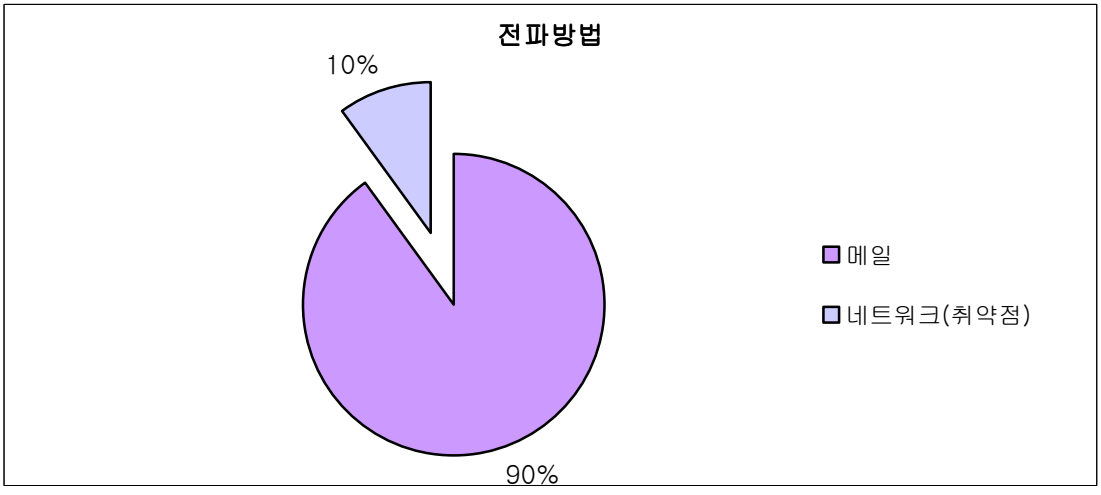
11월의 악성코드 피해 Top 10을 도표로 나타내면 [그림1]과 같다



[그림1] 2004년 11월 악성코드 피해 Top 10

11월 악성코드 Top 10 전파방법별 현황

[표1]의 Top 10 악성코드들은 주로 어떠한 감염경로를 가지고 있는지 [그림2]에서 확인할 수 있다.



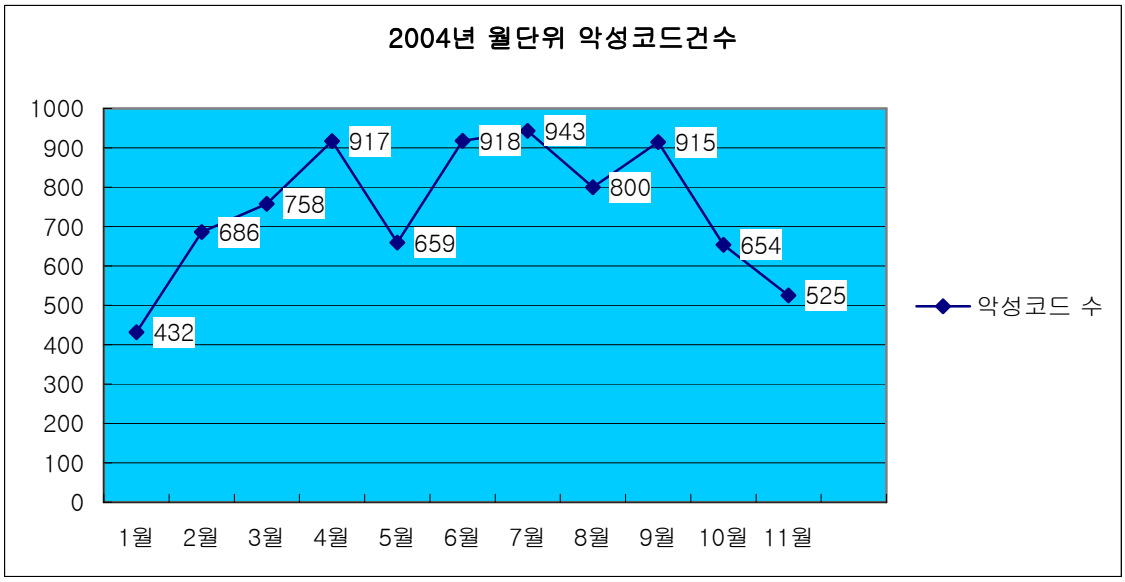
[그림2] 악성코드 Top 10의 전파방법별 현황

Top 10을 차지하고 있는 악성코드의 성격만으로 볼 때 보안취약점을 이용해 네트워크로 전

파되는 새서 웜 이외에는 모두 메일로 전파되는 악성코드들인 것을 알 수 있다. 이것은 피해 집계를 통한 Top 10일 뿐이며 메일로 전파되는 악성코드가 네트워크의 보안취약점을 이용한 악성코드보다 우위에 있다고 판단하여서는 안되겠다.

월별 피해신고 악성코드 건수 현황

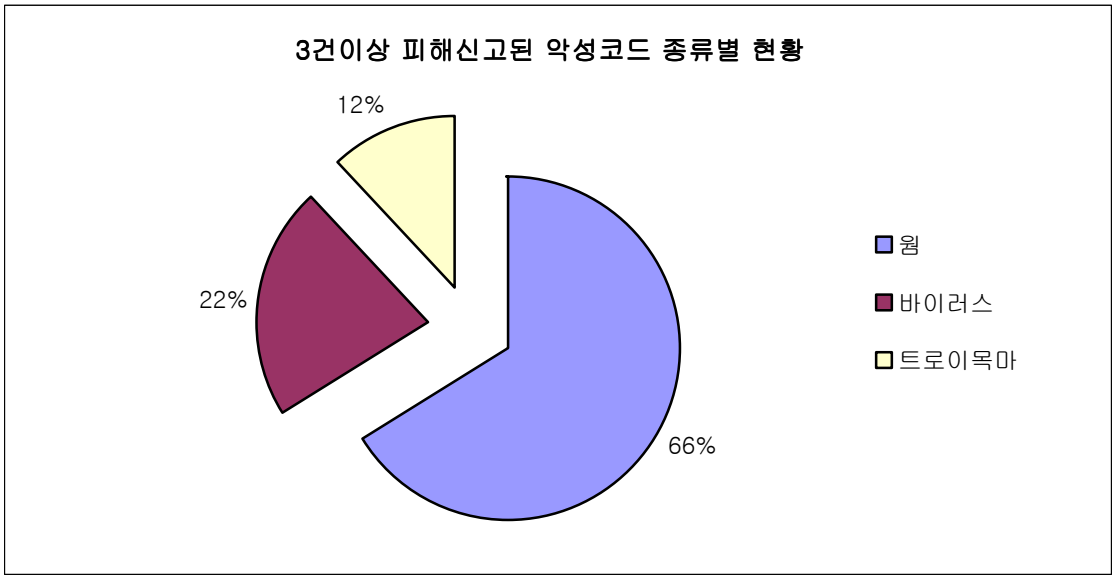
11월에 피해 신고된 악성 코드는 525개이다. 그래프상의 수치로 볼 때 올 1월의 432건 이후 가장 적은 신고건수 임을 [그림3]에서 확인할 수 있다. 이 같은 감소추세는 악성 아이알씨봇에 대한 V3엔진의 진단/치료 기능 강화가 가장 큰 영향을 끼친 것으로 판단된다.



[그림3] 2004년 월별 피해신고 악성코드 수

주요 악성코드 현황

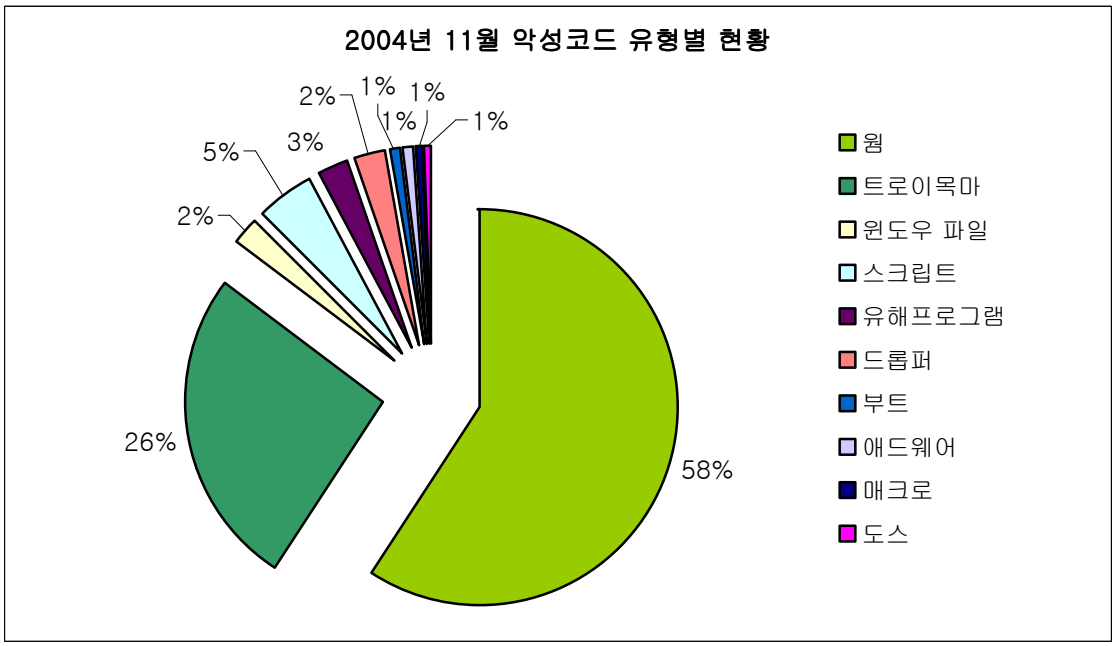
11월에 피해가 접수된 악성코드 중 3건 이상의 문의가 들어온 악성코드의 종류는 [그림4]와 같다.



[그림4] 3건 이상 피해 신고된 악성코드 종류별 현황

웜이 66%(39개)로 가장 많았으며 바이러스 22%(13개), 트로이목마 12%(7개)의 순이다. 바이러스나 트로이목마의 점유율이 증가한 것으로 보이나 이는 전체적인 피해신고 건수가 줄어듬에 따라 나타난 변화이다.

악성코드 유형별 현황은 [그림5]와 같다.



[그림5] 악성코드 유형별 현황

11월의 악성코드 피해건수에 비해 신고된 악성코드수는 눈에 띄게 감소하였다. V3엔진의 강화에 따른 신고건수의 감소는 고무적이라 할 수 있다. 다만 아직까지도 메일을 통해 전파되는 악성코드의 피해건수가 줄어들지 않고 있는 점과 11월에 급격히 줄어들기는 했으나 예년과 비교했을 때 전반적으로 많이 발견된 보안취약점을 이용하여 네트워크로 전파되는 악성코드가 계속 발견되고 있다는 점은 꼭 기억하여 상황에 적절한 대응을 지속적으로 수행해 나가야 할 것이다.

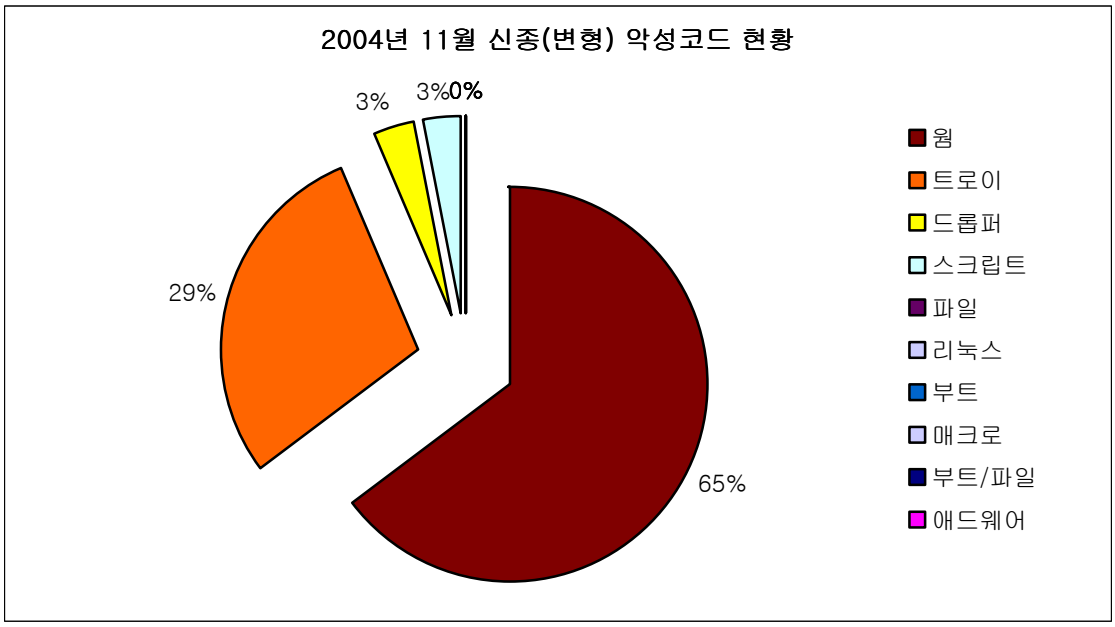
Ⅱ. 11월 국내 신종 악성코드 발견 동향

작성자 : 최동균 연구원(cdk@ahnlab.com)

11월 한달 동안 접수된 신종(변형) 악성코드의 건수는 [표1], [그림1]과 같다.

웜	트로이	드롭퍼	스크립트	파일	리눅스	부트	매크로	부트/파일	애드웨어	합계
213	95	11	10	0	0	0	0	0	0	329

[표1] 2004년 11월 유형별 신종(변형) 악성코드 발견현황



[그림1] 2004년 11월 신종 악성코드 발견현황

11월 신종 악성코드 동향

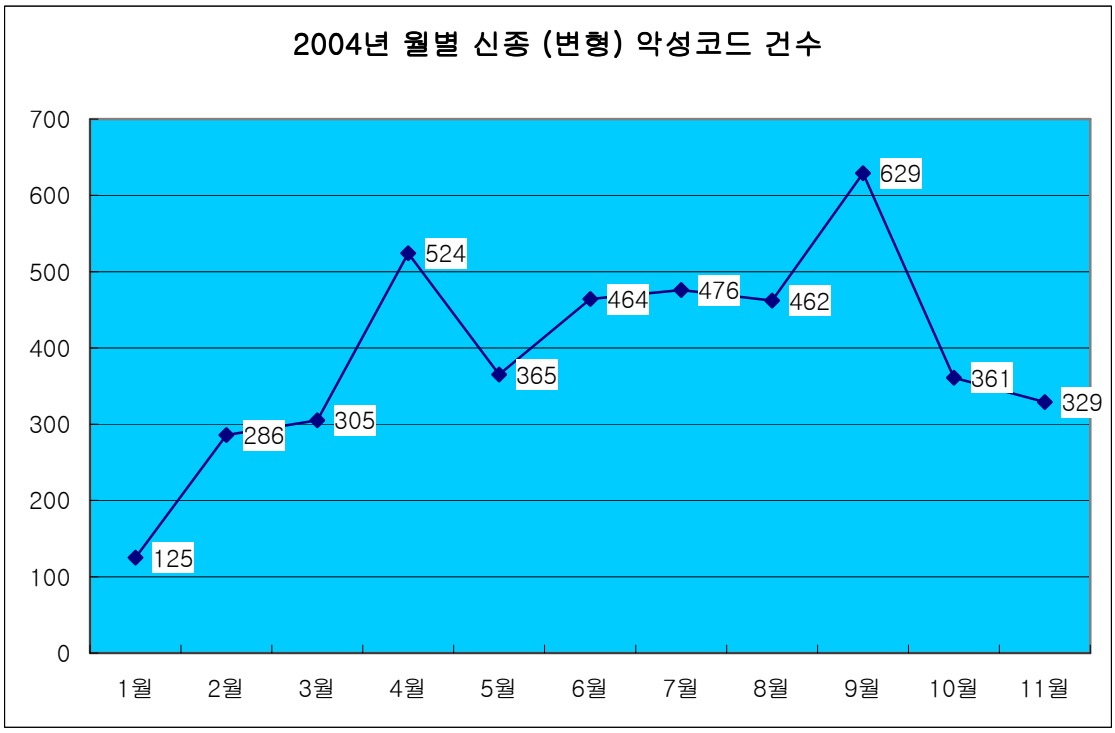
11월 크게 주목할 사항은 Zero-Day Exploit Attack을 위한 악성코드가 발견, 보고되었다는 점이다.

인터넷 익스플로러 6.0 브라우저에서 검사되지 않은 iframe 태그로 인한 버퍼오버플로우 발생 가능성이 11월 5일 포럼 등을 통해 언급되었으며, 해당 취약점을 이용한 악성코드인 보프라 웜(Win32/Bofra.worm.20751)[1]이 11월 9일 발견되었다. 이는 보안 취약점 공개 후 이를 이용한 악성코드 제작까지의 소요시간이 비교적 여유가 있었던 기존의 통념을 무너뜨리는 것으로 마이크로소프트사는 보안취약점 정기업데이트 예정일인 12월 7일 보다 앞당겨서 12월 1일 해당 취약점을 보완하기 위한 패치를 제공하였다.

MS의 윈도우 보안취약점은 악성코드 제작자들에게 충분히 매력적인 소재임에 틀림없다. 이

[1] 타백신에서는 MYDOOM 으로 명명되기도 한다

를 이용한 악성코드는 앞으로 꾸준히 증가할 것으로 예상되며, Zero-Day Exploit Attack 피해 방지를 위해 관련 시스템의 보안패치 배포시 즉시 적용하는 등의 적극적인 관심이 필요하다.



[그림2] 2004년 월별 신종(변형) 악성코드 발견 현황

이번 달에 변형 및 새로이 발견, 보고된 악성코드중 이슈가 있었던 것은 다음들과 같다.

▶ 보프라 웜(Win32/Bofra.worm.20751)[1]

인터넷 익스플로러의 보안 취약점(MS04-040)[2]을 이용하며, 이메일을 통해 전파되어 감염 시스템이 크게 확산되었다.

보프라 웜은 발송되는 이메일 헤더를 변조하여 백신프로그램에서 검증된-감염되지 않은 메일-것처럼 사용자를 현혹하여 감염을 유도한다. 변조하는 이메일 헤더 내용은 다음과 같은 유형이다.

- X-AntiVirus: Checked by Dr.Web (http:/ /www.drweb.net)
- X-AntiVirus: scanned for viruses by AMaViS 0.2.1 (http:/ /amavis.org/)

[1] AhnLab, Win32/Bofram.worm.20751
http://info.ahnlab.com/smart2u/virus_detail_1584.html

[2] Micorsoft, 인터넷 익스플로러 6.0 SP1의 IFRAME SRC NAME 버퍼 오버플로우 보안문제 (MS04-040)
http://www.microsoft.com/technet/security/bulletin/MS04-040.mspx (영문자료)
http://www.microsoft.com/korea/technet/security/bulletin/MS04-040.mspx (한글자료)

- X-AntiVirus: Checked for viruses by Gordano's AntiVirus Software

이메일 본문 중 IFRAME 태그에서 버퍼오버플로우를 발생하여 악의적인 사용자가 Administrator 권한을 획득할 수 있다. 따라서 해당 취약점에 대해 시스템을 보호하기 위해서는 관련 보안패치를 적용하거나, 윈도우 XP 사용자는 DEP(Data Execution Protection) 기능이 포함된 서비스팩 2 설치해야 한다.

보프라 웜은 이 웜이 이용하는 취약점이 공개된 이후 불과 4일만에 발견되었다. 이는 Zero-Day Exploit Attack의 주기가 점점 단축되고 있으며, 악성코드 제작자들이 시스템 감염을 위해 언제든 최신 보안취약점을 이용할 수 있음을 시사하고 있다.

▶ 모페이 웜(Win32/Mofei.worm.23552)[1]

WMF(Windows Metafile) 및 EMF(Enhanced Metafile) 이미지 형식의 파일을 처리하는 그래픽 렌더링 엔진에서 발생할 수 있는 취약점(MS04-032)[2]을 이용한 악성코드가 발견 되었다.

보안에 취약한 시스템이 해당 취약점 코드를 가지고 있는 이메일 열람시 Heap Overflow 를 발생하여 악의적인 사용자가 Administrator 권한을 획득할 수 있다. 취약점에 대해 시스템을 보호하기 위해서는 관련 보안패치를 적용하거나, Windows XP 사용자는 서비스팩2 설치를 권장한다.

해당 취약점의 대상이 .EMF 확장자의 32bit 이미지 형식 파일의 처리가 가능한 Windows XP 시스템으로 한정되어 있고 취약점에 의해 유발되는 Heap Overflow 는 관련된 필수 특정 DLL 의 메모리 주소가 동적으로 할당 되어 시스템별 정상동작(Heap Overflow 유발)을 가늠하기 어려운 형태여서 감염피해 규모는 크지 않았다.

하지만 취약점을 포함한 이미지 파일 제작이 비교적 단순하여 다수의 변종이 출현할 가능성이 있으니, 대상 시스템은 취약점에 노출되지 않도록 관련 보안패치 적용을 권장한다.

▶ 스컬스(Skulls)

모바일폰에 탑재되어 사용되는 운영체제인 심비안(Symbian) OS를 감염시키는 스컬스의 변형이 발견되었다.

이는 테마 매니저를 가장한 'icons.sis' 파일을 모바일폰에 다운로드할 때 감염되며, 대표적인

---

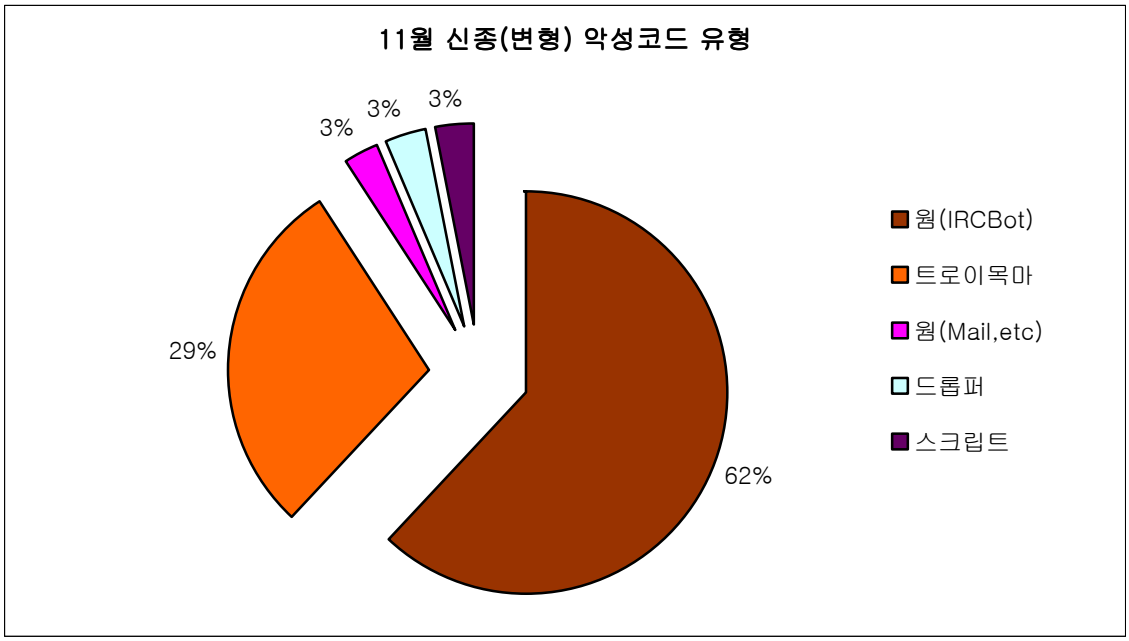
[1] AhnLab, Win32/Mofei.worm.23552
http://info.ahnlab.com/smart2u/virus_detail_1593.html

[2] Microsoft,, 그래픽 렌더링 엔진 취약점(MS04-032)
http://www.microsoft.com/technet/security/bulletin/ms04-032.mspx (영문자료)
http://www.microsoft.com/korea/technet/security/bulletin/ms04-032.mspx (한글자료)

증상은 모든 메뉴 아이콘이 해골(Skull)로 변하고 통화 이외의 부가기능은 사용할 수 없게 된다. 또한 감염대상 블루투스 디바이스를 지속적으로 탐색하는 증상으로 인해 모바일폰 배터리 사용 시간이 단축될 수 있다.
더불어 블루투스를 통한 복제 바이러스 자동전파 가능성이 제기되었으나, 감염대상 시스템(모바일폰)사용자가 외부로부터 유입된 프로그램 설치에 승인하는 절차가 필요하여 2차 감염 우려는 없는것으로 확인되었다.
스컬스는 심비안 OS를 사용하는 모바일폰으로 감염대상이 한정되어 있으며, 2차 감염에 대해 사용자의 개입(실수)을 필요로 하여 자체가 가지는 파괴력은 미미하다. 하지만 악성코드 제작자들의 감염목표가 데스크탑에 국한되지 않고 휴대용 기기 등으로 확장 중이며, 모바일 악성코드를 악의적인 목적으로 연구하는 활동이 증가하고 있음을 시사하고 있다.

유형별 신종(변형) 악성코드 현황

다음은 11월 발견된 신종(변형) 악성코드의 유형별 현황이다.



[그림3] 11월 신종(변형) 악성코드 유형별 현황

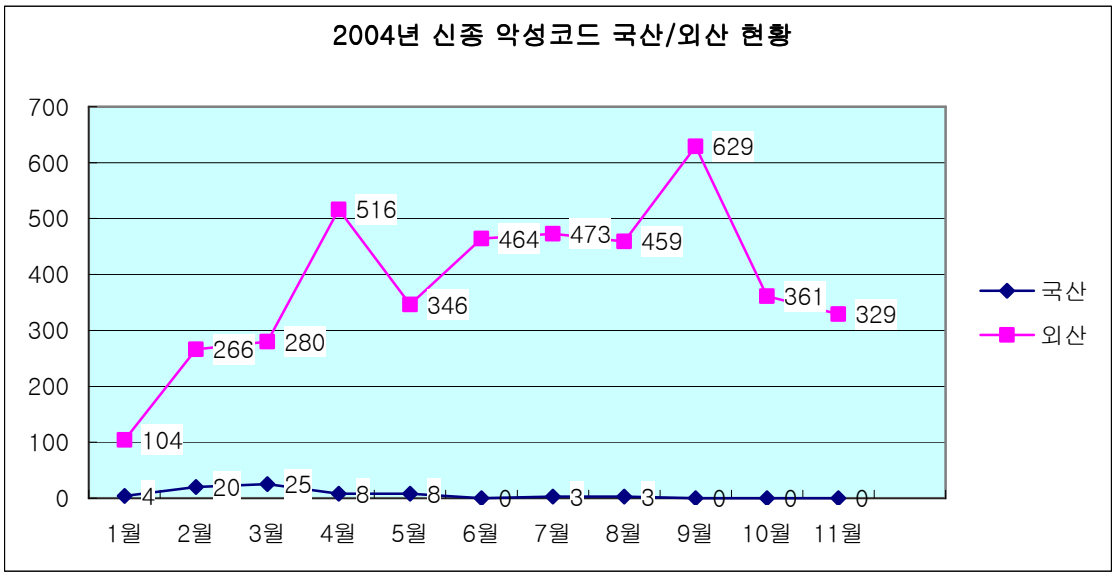
지난달에 기술한 것처럼 샘플접수관련 정책이 변경되어 기존 진단된 악성 아이알씨봇(IRCBot) 웜 유형은 신종(변형)의 악성코드 집계에서 제외되어 악성 아이알씨봇(IRCBot) 웜이 차지하는 비중이 10월에 이어 감소 추세를 보이고 있다. 하지만 타 악성코드 유형에 비해 상대적인 비중은 여전히 매우 높은 것을 알 수있다.

전통적인 악성코드 유형 중 시스템 감염 후 독립적인 임무를 수행하는 객체를 다수 내포하고 있는 드롭퍼의 발견이 조금씩 증가를 보이고 있다. 이로인해 감염된 시스템은 리소스 부

족, 백도어 오픈, 네트워크 트래픽 증가 등의 복합적인 증상이 나타난다.

제작지별 신종(변형) 악성코드 현황

다음은 신종(변형) 악성코드들의 국산/외산 현황이다.



[그림4] 2004년 제작지별 신종 악성코드 현황

11월 신종 악성코드의 제작지는 모두 국외로 확인되었으며, 국내의 경우 애드웨어 및 스파이웨어의 제작이 눈에 띈다. 이들의 차이점은 악성코드 대부분이 시스템 장악 및 능률성 저하를 목적으로 하는 반면 애드웨어 및 스파이웨어의 경우 통상 금전적 이득을 목적으로 제작되는 특성이 있다.

향후 악성코드 제작 유형별 비중은 큰 변화를 보이지 않고 여전히 국외에 편중된 양상을 나타낼 것으로 전망된다. 애드웨어 및 스파이웨어의 경우 이에 대응하는 제품들을 우회하기 위해 점점 지능화되고 있어 악성코드와의 경계가 옅어지고 있다. 이는 현재 서로 분리된 영역의 전통적인 백신프로그램과 안티 애드웨어의 통합화가 필요하다는 것을 의미한다고 할 수 있다.

또한 올 한해 악성코드 키워드 중 하나였던 봇류가 하향 곡선을 그리고 있어, 이를 대체하기 위한 새로운 유형의 악성코드가 출현할 가능성이 있음을 예의 주시할 필요가 있다.

III. 11월 신규 보안취약점

작성자 : 이정형 연구원(jungh@ahnlab.com)

11월달에는 이전달에 비하여 보안패치 발표가 가장 적었던 달이다. 11월달에 발표된 취약점은 ISA Server 2000 및 Proxy Server 2.0의 취약점으로 인한 인터넷 콘텐츠 스푸핑 허용 문제(MS04-039)와 인터넷 익스플로러 6.0 SP1의 IFRAME SRC NAME 버퍼 오버플로우 보안문제(MS04-040)가 있었다. 이중에서 인터넷 익스플로러의 버퍼오버플로우 문제를 알아보기로 하자.

개요

이 취약점은 IFRAME, FRAME, EMBED 요소에서 사용되는 SRC와 NAME 속성에 최대 버퍼크기보다 큰 값이 들어갈 때 버퍼오버플로우가 발생하여 악의적인 침입자가 해당 시스템을 장악할 수 있는 버그이다.

이번 취약점에 영향을 받는 소프트웨어는 다음과 같다.

Microsoft Internet Explorer 6.0 SP1 가 포함되어있는 운영체제
Windows 98
Windows 98 Second Edition
Windows Me
Windows 2000 SP3
Windows 2000 SP4
Windows NT 4.0 Server SP6a
Windows NT 4.0 Server TSE SP6
Windows XP 64-bit Edition SP1
Windows XP SP1

취약점 설명

IFRAME이란 Inline Floating Frame의 줄임말로써, 웹문서안에 추가로 웹문서를 포함할 때 사용되어지는 태그이며, 해당하는 속성들은 다음과 같다.

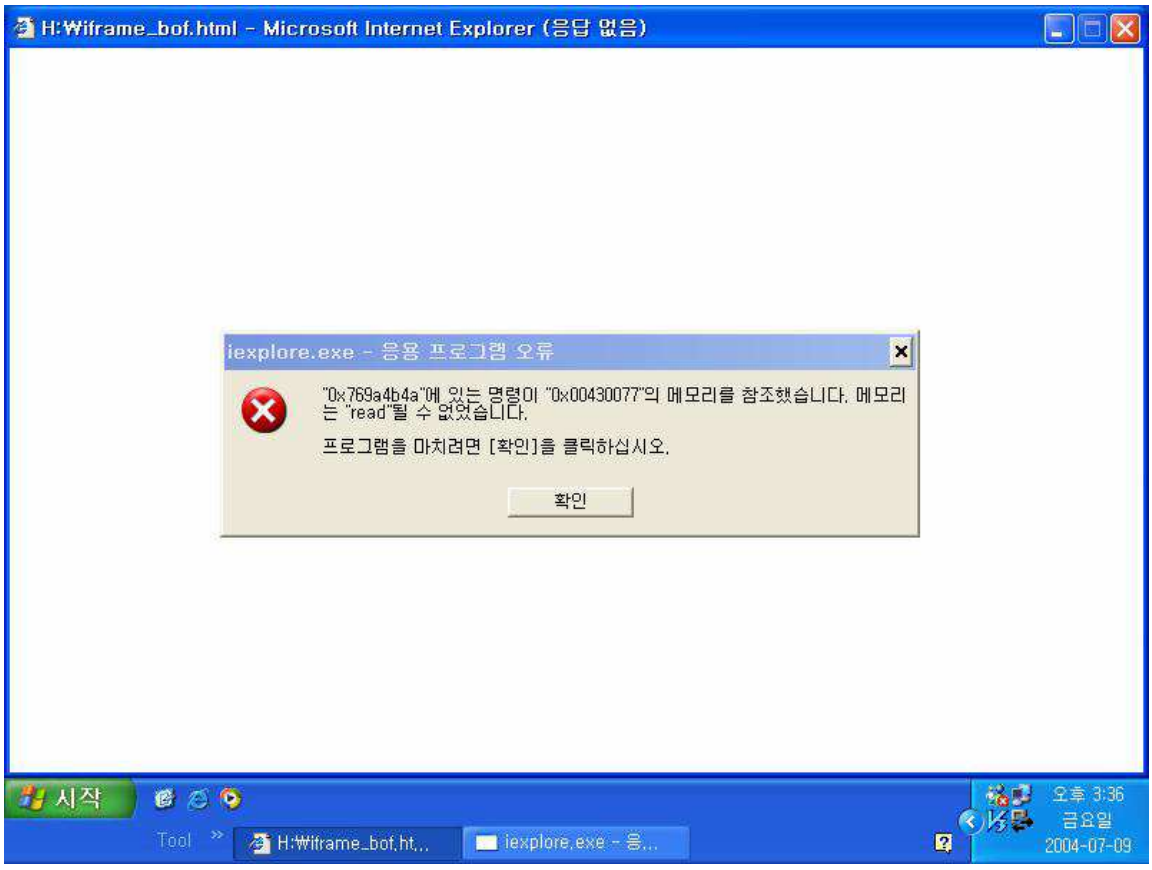
속성	설명
Src	프레임속에 보여질 문서의 주소
Name	이름, 프레임 태그의 name
Width	프레임의 넓이
Height	프레임의 높이

marginwidth	프레임의 좌우 넓이
magrinheight	프레임의 상하 여백
Frameborder	프레임 border 의 두께
Align	정렬방식
Scrolling	스크롤바 생성 여부
Hspace/vspace	가로, 세로 여백

SRC와 NAME 속성에 아래와 같은 조건일 경우에 버퍼오버플로우가 발생하게 된다.

<IFRAME SRC=file://A x 250 (250 bytes 이상)
NAME="A x 2024 (2024 bytes 이상)"> </IFRAME>

아래 그림은 버퍼오버플로우가 발생하였을 때 인터넷 익스플로러의 화면이다.



이 취약점은 사용자가 웹 사이트에서 취약점 코드가 내장된 악의적인 웹페이지를 보거나 취약점 코드가 포함된 HTML 문서를 볼 때 시스템 관리자의 권한을 빼앗길 수도 있다.
공격코드가 11월 초에 언더그라운드 메일링 리스트에서 발표되면서 애드웨어와 메일의 첨부

파일을 사용하지 않는 보프라 웜(Win32/Bofra.worm)[1]에서 벌써 이 취약점을 이용하여 피해를 주고 있다.

웜과 애드웨어, 다운로더 등에서 취약점 코드가 내장이 되어있는 웹 문서에 접속하게 하거나, 파일 다운로드, 파일이 첨부되는 형태로의 공격방법이 예상되며, 이를 통해 임의적으로 악성 프로그램을 실행을 할 수 있으니 주의가 요망된다.

이 취약점에 해당하는 보안패치는 취약점이 공개된지 한달 후인 12월 초에 마이크로소프트사에서 발표되었다.[2]

브라우저 보안

브라우저에서 늘 문제가 많이 되는 것은 ActiveX와 JavaScript이다. 보안 설정에서 이 기능을 해제하고 사용하면 보안에 많은 도움이 되지만, 일반적인 사이트들에 접속했을 때 웹페이지가 제대로 안보이는 문제점이 있다.

웹 브라우저인 인터넷 익스플로러에는 많은 취약점들이 존재하며, 그중에서는 패치가 되지 않은 취약점들 또한 존재한다. 인증된 사이트 또는 공식 사이트들만 접속하는 것이 가장 좋으며, 기타 브라우저인 파이어폭스(모질라)등을 사용하는 것도 한가지 방법일 수 있다.
마지막으로 보안이 강화된 윈도우 XP 서비스팩 2 버전을 사용을 하여도 많은 취약점 공격으로부터 벗어날 수 있다.

---

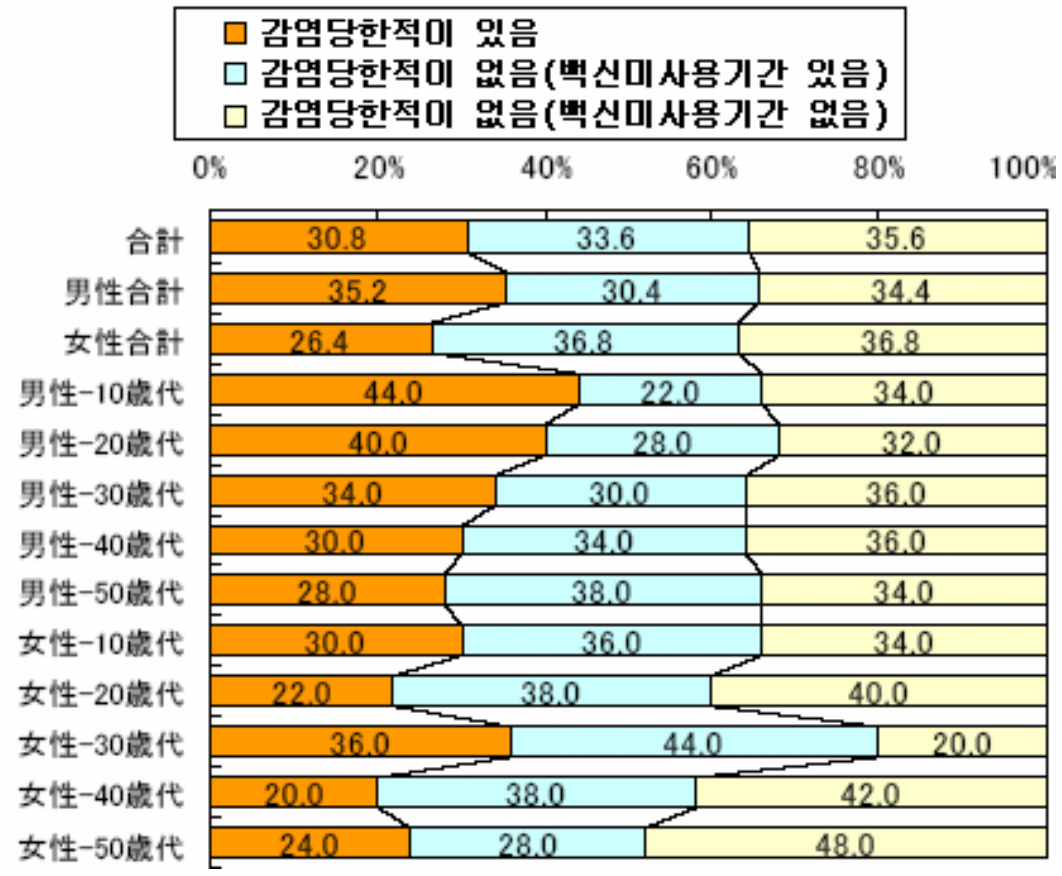
[1] AhnLab, 보프라 웜
http://info.ahnlab.com/smart2u/virus_detail_1584.html

[2] 마이크로소프트, MS04-040 :
http://www.microsoft.com/technet/security/bulletin/MS04-040.mspx

Ⅳ. 11월 일본 피해 동향

작성자 : 김소헌 주임연구원(sohkim@ahnlab.com)

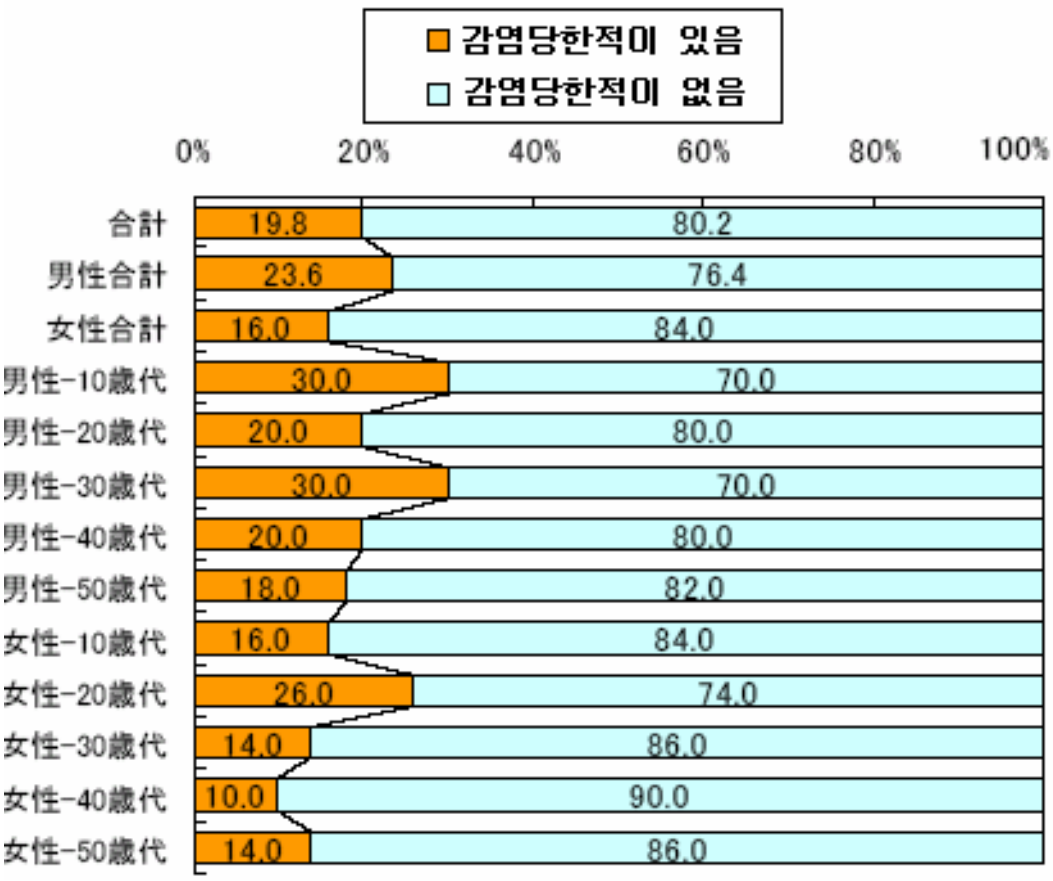
일본의 마케팅 관련 회사인 Cyber Brains(http://www.cyber-brains.com)가 일본의 백신프로그램 이용현황을 조사한 자료에 따르면 일본 PC 사용자의 백신 프로그램 사용률은 73.5%이고 이중 악성코드에 감염된 경험이 있는 PC 사용자는 30%정도인 것으로 나타났다. [그림1]은 악성코드 감염 경험 여부를 묻는 항목에 대한 피설문자의 응답 내용을 도표로 나타낸 것이다. 타 연령대에 비해 10대와 20대 남성의 악성코드 감염 경험이 가장 많은 것을 알 수 있는데, 이는 타 연령대에 비해 PC 사용량이 많고 업무 이외의 용도로 사용되는 경우가 많은 것이 원인이 될 수 있을 것이다.



[그림1] 백신프로그램 설치 전 악성코드 감염 경험 여부 조사 (자료출처 : Cyber Brains)

[그림2]는 백신 프로그램 설치 후 악성코드에 감염된 경험이 있는지 여부를 묻는 항목에 대한 피설문자의 응답 내용이다. 조사결과 감염을 당한 경험이 있는 피설문자가 20% 정도로 높게 나타났는데 이러한 현상은 제작 기법이 다양해지고 OS에 대한 직접적인 공격이 빈번하게 발생하는 등 빠르게 진화하는 악성코드들로부터 백신 프로그램이 PC 사용자의 안전을 보

장해주는 것에 한계가 있음을 보여주는 것이라 할 수 있다.



[그림2] 백신프로그램 설치 후 악성코드 감염 경험여부 조사 (* 자료출처 : Cyber Brains)

물론 백신 프로그램 제작업체에서도 이러한 상황을 극복하기 위해 방화벽과 같은 여러 가지 보완 제품들이 배포되고 있으나 아직 PC 사용자들은 이러한 잠재된 위협에 대해서는 아직 둔감한 것으로 보인다.

일본 유행 악성코드 유형별 발생현황

2004년 11월 한달 동안 일본에서 가장 많이 유행한 악성코드는 전월과 마찬가지로 넷스카이 웜(Win32/ Netsky.worm)이다.

[표1]은 일본의 IPA/ISEC에서 집계한 2004년 12월 악성코드 피해 통계자료이다. 넷스카이 웜의 피해 신고 건수가 1,315건으로 가장 많은 양을 차지하고 있는 것을 볼 수 있다.

[표1]에는 포함되어 있지 않지만 11월에 새롭게 제작되어 확산된 보프라웜(Win32/Bofra.worm)이 40건을 기록하고 있다.

Window/Dos Virus	건수	Macro Virus	건수	Script Virus	건수
W32/Netsky	1,315	Xm/Laroux	27	VBS/Redlof	92
W32/Bagle	654	X97M/Tristate	10	VBS/ Fortnight	7
W32/Mydoom	394	W97M/Melissa	4	VBS/Loveletter	4
W32/Lovgate	322	X97M/Divi	3	VBS/FreeLink	3
W32/Klez	310	WM/Sic	3	VBS/Netlog	3
W32/Zafi	211	W97M/Ethan	2	VBS/ Internal	2

[표1] 11월 일본의 악성코드 피해 신고 현황(출처: IPA/ISEC)

악성코드의 감염 경로별 통계

[표2]는 감염된 악성코드의 감염 경로에 대한 통계를 나타낸 것이다. 표에서 알 수 있는 것처럼 메일을 통한 감염이 98.5%로 감염의 주요 경로인 것을 알 수 있다.

한해 동안 발견되는 악성코드들 중에서 Mass Mailer의 기능을 가진 악성코드가 차지하는 비율은 매우 적다. OS나 아웃룩 등의 취약점을 이용하는 특별한 경우를 제외하고는 사용자가 직접 파일을 실행시켜야 하는 등 조금만 조심하면 감염을 막을 수 있는 이메일 웜의 특성을 생각해 볼 때 감염 예방을 위한 사용자의 주의가 필요하다고 할 수 있다.

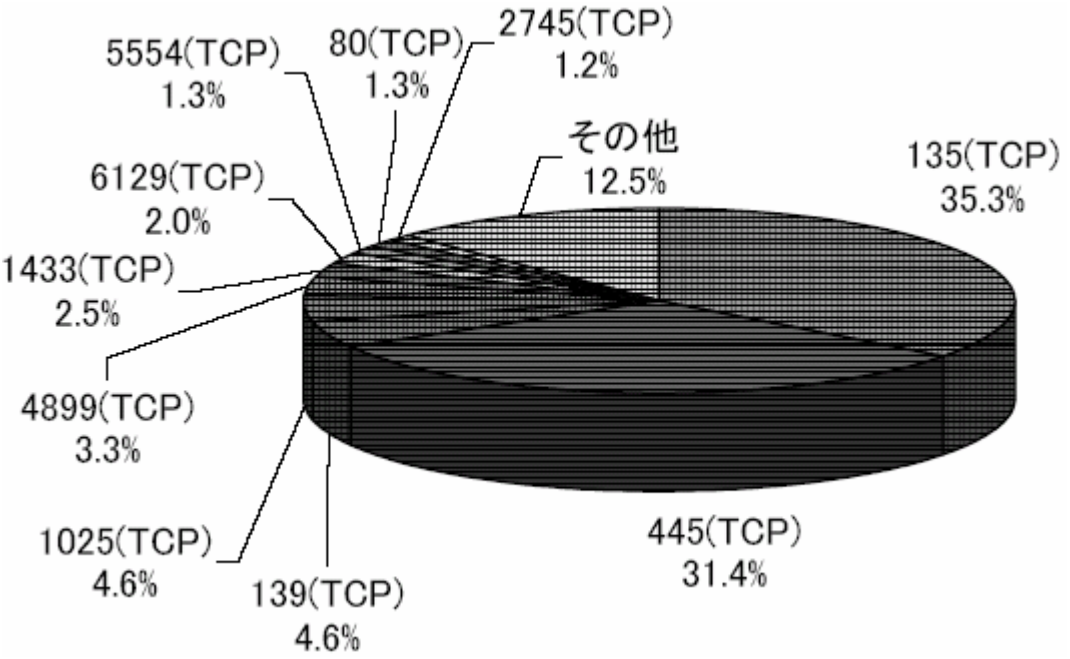
감염경로	피해 건수					
	2004년 10월		2004년 9월		2003년 10월	
메일	5,229	98.5%	4586	98.5%	1,650	92.4%
외부의 모체	3	0.1%	1	0%	20	1.1%
다운로드	5	0.1%	6	0.1%	4	0.2%
네트워크	62	1.2%	51	1.1%	60	3.4%
기타	9	0.2%	10	0.2%	52	2.9%

[표2] 악성코드 감염 경로 통계

일본 네트워크 트래픽 현황

[그림3]은 2004년 11월 일본의 네트워크 트래픽 현황을 표로 나타낸 것이다.

가장 많은 트래픽이 발생한 포트는 TCP 135와 TCP 445 포트이다. 두 포트들은 윈도우에서에서 기본으로 사용되는 포트들이지만 최근에는 아고봇(AgoBot)과 같은 네트워크를 통해 전파되는 웜들이 윈도우의 취약점을 이용한 공격 시 사용되는 경우가 많다. OS가 알 수 없는 이유로 재시작되거나 외부로 대량의 트래픽을 유발하는 경우 해당 취약점을 이용한 웜에 감염되었을 가능성이 매우 높으므로 백신 프로그램을 이용할 것을 권장한다.



[그림3] 일본의 네트워크 트래픽 현황

V. 11월 중국 피해 동향

작성자 : 장영준 연구원(zhang95@ahnlab.com)

2004년 한해도 어느덧 저물어 가고 2005년 새해를 맞이하는 12월에 이르렀다. 2004년 한해를 마무리하는 중국 현지에서는 11월 한달 동안 어떠한 악성코드들이 발견되고 많은 확산이 되었는지 짚어보도록 하자.

악성코드 TOP 5

순위 변화	순위	Rising
-	1	Worm.Lovgate
-	2	Worm.Netsky
↑ 1	3	TrojanDroper.Worm.Bagz
↓ 1	4	Backdoor.Rbot
-	5	Backdoor.Sdbot

[표1] 2004년 11월 Rising 악성코드 TOP 5

'-' - 순위변동 없음, 'New' - 순위에 새로 진입, '↑'- 순위 상승, '↓' - 순위 하락

순위 변화	순위	CNCVERC
-	1	Worm_Netsky.D
-	2	Worm_Lovegate.C
-	3	Worm_Bbeagle.J
-	4	Worm_AgoBot

[표2] 2004년 11월 CNCVERC 악성코드 TOP 4

'-' - 순위변동 없음, 'New' - 순위에 새로 진입, '↑'- 순위 상승, '↓' - 순위 하락

위 [표1]은 중국 로컬 안티바이러스 업체인 라이징(Rising)사에서 조사한 11월 한달 동안 가장 많은 감염 신고가 있었던 악성코드 순위이다. 지난 10월과 비교하여 가장 두드러진 변화는 백쯔 웜(TrojanDroper.Worm.Bagz, V3진단명 Win32/Bagz.worm.155140)이 큰 폭으로 증가하였다는 것이다. 그 증가폭은 이번 달에도 1위와 2위를 차지하고 있는 러브게이트 웜 (Worm.Lovgate, V3진단명 Win32/Lovgate.worm)과 넷스카이 웜 (Worm.Netsky , V3진단명 Win32/Netsky.worm)의 수치를 위협하는 수위에 이르고 있다. 이러한 백쯔 웜의 증가세로 인해 아이알씨봇 웜(Backdoor.Rbot, V3진단명 Win32/IRCBot.worm)은 한계단 하락하게 되었다. 이 두 웜의 변화를 제외하고는 지난 10월달과 비교하여 동일한 순위를 유지하고

있다. 그리고 [표2]는 중국국가컴퓨터바이러스대응중심(China National Computer Virus Emergency Response Center – 이하 CNCVERC)에서 작성한 11월 한달 동안의 순위이다. 위 표에서와 같이 이번 11월달에도 10월달과 같이 순위 변화없이 현상 유지를 보여주고 있다. 이러한 라이징과 CNCVERC의 순위차이는 데이터 수집과 통계 작성 방식의 차이로 볼 수 있다.

주간 악성코드 순위

순위	1주	2주	3주	4주
1	Worm.Netsky	Worm.Lovgate	TrojanDroper.Worm.Bagz	Backdoor.Rbot
2	Worm.Lovgate	TrojanDroper.Worm.Bagz	Worm.Netsky	Backdoor.Sdbot
3	TrojanDroper.Worm.Bagz	Worm.Netsky	Worm.Lovgate	TrojanDroper.Worm.Bagz
4	Worm.BBeagle	Backdoor.Rbot	Worm.Agobot	Trojan.PSW.Lieage
5	Backdoor.Rbot	Worm.Agobot.3	Backdoor.Rbot	Worm.Netsky

[표3] 2004년 11월 Rising 주간 악성코드 순위

순위	1주	2주	3주	4주
1	Worm_Netsky.D	Worm_Netsky.D	Worm_Netsky.D	Worm_Netsky.D
2	Worm_Lovgate.C	Worm_Bbeagle.J	Worm_Bbeagle.J	Worm_Lovgate.C
3	Worm_Bbeagle.J	Worm_Lovgate.C	Worm_Lovgate.C	Worm_Bbeagle.J
4	Worm_AgoBot	Worm_AgoBot	Worm_AgoBot	Worm_AgoBot

[표4] 2004년 11월 CNCVERC 주간 악성코드 순위

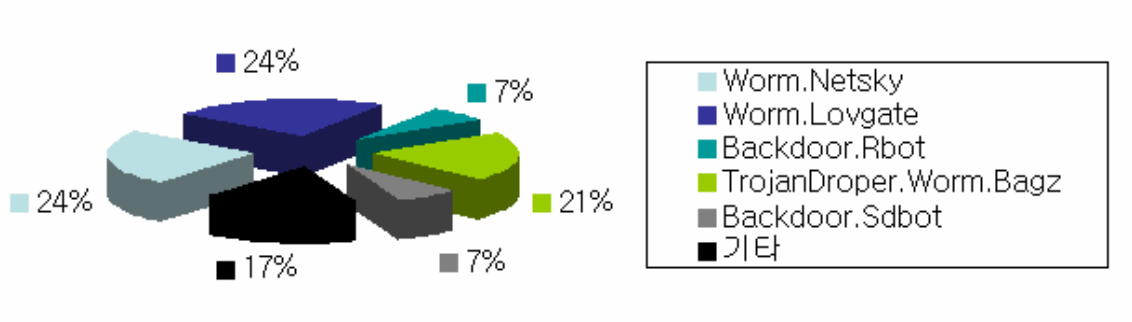
[표3]의 라이징 주간 악성코드 순위 변화를 살펴 볼 경우에도 백쯔 웜의 증가세가 잘 반영되어 있다. 특히 11월 3주차에서는 기존의 넷스카이 웜과 러브게이트 웜을 제치고 1위를 차지할 만큼 급상세를 타기도 하였다. 그러나 4주차에 접어 들면서 감소세를 보여 3위로 하락하였다. 이러한 순위하락이 일시적인 현상일지 아니면 12월 1주차에서 다시 상승세로 이어갈지는 상당히 주목할 부분이다. 그리고 11월 주간 악성코드 순위에서 트로이목마로서는 유일하게 4주차에 Trojan.PSW.Lineage가 등장하기도 하였다.

신종 악성코드 동향

11월에 발견된 신종 악성코드는 트로이목마의 강국이라는 중국답게 대부분 백도어 또는 트로이목마류였다. 그러나 그 중에서 유일하게 I-Worm.TachQQ만이 메일을 전파경로로 이용하는 메스메일러(Mass Mailer)였다. I-Worm.TachQQ는 비주얼 베이직 5.0으로 제작되었으며 실행압축된 형태였다. 그리고 발신되는 메일주소는 @qq.com로 되어있으며 전파되는 메일 형식도 모두 중국어로 된 점이 특이할 만하다. 그리고 이번 달 역시 QQ 메신저를 이용하여 전파되는 트로이목마인 Trojan.QQMSG.Boker가 발견된었다. Trojan.QQMSG.Boker는

QQ 트로이목마의 전형적인 형태로 QQ 메신저를 이용하여 특정 웹 사이트로 접속을 유도하는 문구를 전송한다. 그리고 해당 웹 사이트에 접속하게 될 경우, 해당 트로이목마가 감염되는 형태이다.

악성코드 분포



[그림1] 2004년 11월 중국의 악성코드 분포

이번 달의 악성코드 분포의 특징은 글머리에서 서술한 바와 같이 백쯔 웜의 급격한 증가세라 할 수 있다. 백쯔 웜을 지난 달의 분포와 비교해 볼 경우 지난 10월 7.6%였었으나 이번 달에는 3배 가량 증가한 21%로 대폭 증가하였다. 이 수치는 이번 달 순위에서 1위와 2위를 차지하고 있는 러브게이트 웜과 넷스카이 웜의 분포와 거의 비슷한 수위까지 이르게 되었다는 것을 [그림1]에서 자세히 보여주고 있다. 이에 반해 지난 달 36%와 30%였던 러브게이트 웜과 넷스카이 웜은 10% 가량 감소한 24%를 보여 주고 있다. 이러한 두 웜의 감소 현상은 백쯔 웜의 증가세도 한 요인으로 작용하였지만 기타에 포함된 다양한 악성코드의 등장으로도 기인한다고 볼 수 있다. 기타에 포함된 악성코드들로는 베이글 웜(Worm.Bbeagle, V3 진단명 Win32/Bagle.worm), Trojan.StartPage.Sexplorer, I-Worm.TachQQ와 Backdoor.Banito.plugin 등 다양한 종류의 악성코드들이 포함되어 있다.

맺음말

11월달의 가장 큰 변화는 글 머리에서 언급한 것과 같이 백쯔 웜이 기존의 러브게이트 웜과 넷스카이 웜의 수치에 이를 만큼 널리 확산된 것으로 분석된다. 특히 10월 마지막 주에 등장하여 한달 사이 기존의 웜 수치만큼 증가하였다는 것은 중국 현지에서의 확산이 한국이나 유럽권에 비하여 특히나 많은 감염이 있었던 것으로 추정된다. 그리고 또 하나의 특이점을 짚어 볼 경우, 다양한 형태의 악성코드가 대거 등장했다는 것이다. 기존의 중국 악성코드 동향은 순위권을 제외한 기타 악성코드 대부분이 트로이목마 또는 백도어류였으나 이번 11월달에는 중국에서 제작 된 것으로 추정되는 메스메일러인 I-Worm.TachQQ, 지속적인 변형이 등장하는 QQ 트로이목마들과 애드웨어 류의 숫적 증가하였다. 이러한 다양한 종류의 악성코드 발견이 향후 중국 악성코드 동향을 어떠한 방향으로 흐르게 될 지 주목된다.